木馬清除大師

用戶手冊

Lofocus 安全實驗室

目　錄

第一章　　木馬清除大師專業版 3

產品描述 3

1・1 產品包構成 3
1・2 產品簡介 3
1・3 木馬清除大師給您帶來的新特性 3
1・4 使用環境： 6

第二章　軟體安裝/移除與在線註冊 7

2・1 軟體安裝： 7
2・2 軟體移除： 10
2・3 軟體註冊： 11

第三章 木馬清除大師軟體使用 12

3・1 木馬清除大師軟體概述 12
3・2 木馬清除大師即時監控簡介 13
3・3 木馬清除大師即時監控設定 17
3・4 木馬清除大師即時監控規則設定 19
3・5 木馬清除大師警告窗口 20
3・6 木馬清除大師主程式設定 24
3・7 木馬清除大師掃瞄介面 27
3・8 木馬清除大師掃瞄硬碟 29
3・9 木馬清除大師掃瞄結果 31
3・10 木馬清除大師進階工具 33
3・11 木馬清除大師智慧升級 40
3・12 木馬清除大師隔離 42

附件一： 44

第一章 木馬清除大師專業版

產品描述

1．1 產品包構成

程式光盤：包含專業版的全部應用程式及產品電子文檔資料。

用戶手冊：即本手冊印刷品，通過閱讀它，掌握本軟體的使用方法和技巧。

1．2 產品簡介

木馬清除大師 (BeatTrojan)是北京 LOFOCUS 安全實驗室爲廣大網路遊戲愛好者及聊天愛好者量身訂做的一款殺毒，殺木馬軟體，到目前爲止已能查殺 X 萬餘種流行木馬、網路遊戲盜號工具、MSN/YAHOO 通盜密碼工具、幽靈後門、流氓軟體及間諜軟體，查殺率在 95%以上。本軟體不僅加強了對系統多個重點區域的檢查，如：登錄檔、Cookies、隱私紀錄、服務、敏感區域等；而且加入了對木馬的啓法式掃瞄，即使木馬能逃脫靜態特徵碼查殺，也無法逃過啓法式掃瞄的雙眼；更有十四大即時監控、即時地保護用戶電腦不受侵害。木馬清除大師完全不同於以前任何版本，除了繼承舊版本的檔案掃瞄引擎外，還包含了全新的用戶介面、全新的即時監控、全新的掃瞄功能及全新的安全防護。

1．3 木馬清除大師給您帶來的新特性

1．3．1 擴充了病毒資料庫，目前已經可以查殺 X 萬餘種有害程式：

●擴展了對盜號木馬的查殺，隨時監控市面上出現的所有網路遊戲盜號木馬，保證第一時間查殺。

●擴展了對流氓軟體的查殺，可以清除目前流行的流氓軟體。

●擴展了對間諜軟體的查殺，可以清除目前流行的間諜軟體，比較典型的是加入了對 Cookie 的查殺。

●擴展了對廣告軟體的查殺，可以清除目前流行的廣告軟體，您不再需要對隨時彈出來的廣告煩心。

1．3．2 新增十四大即時監控：

●可以防止任何有害程式未經允許安裝在用戶電腦上，而不是被動的等中了木馬後，再進行掃瞄清除。

●新增木馬即時攔截

●新增記憶體即時監控

●新增系統資料夾寫入監控

●新增系統資料夾執行監控

●新增登錄檔即時監控

●新增 IE 即時監控

●新增重要系統檔案監控

●新增敏感資料夾即時監控

●新增蠕蟲即時攔截

●新增程式強制終止監控

●新增進程注入監控

●新增網頁木馬監控

●新增木馬側錄監控

●新增 USB 磁碟病毒監控

1．3．3 擴展的掃瞄對像：

●新增對 Cookies 的掃瞄，防止一些間諜 Cookie 洩露您的私人秘密。

●新增對隱私紀錄的掃瞄，防止您的隱私被它人窺探。

●新增硬碟隱蔽區域的掃瞄，防止間諜軟體藏身於此。

1．3．4 增強的掃瞄功能：

●可以對上 20 萬個有害登錄檔項進行安全檢查。

●新增登錄檔深度掃瞄

●大大的提升了記憶體掃瞄的性能，掃瞄速度減半。

1．3．5 增強的病毒隔離功能：

●可以對病毒進行加密隔離，病毒被隔離後將失去危害性。

●在任意地方都進行了隔離，即時監控也可以隔離有害檔案。

●隨時恢復可能被誤刪的檔案。

1．3．6 增強的用戶介面體驗：

●更加友好的用戶介面，即便電腦的初級使用者也能輕鬆使用。

●全新的掃瞄介面，和具備詳細控制和訊息的掃瞄結果。

●未註冊用戶同樣可以看到詳細的掃瞄結果。

1．3．7 人性化的註冊與升級：

●軟體註冊非常便捷，您使用所購買產品包中的授權卡註冊碼訊息或者在線購買軟體註冊碼，並通過在線驗證即完成產品註冊。

●全新智慧升級，自動檢測最新更新，並按照提示操作完成升級。

1．4 使用環境：

1．4．1 硬體環境：

CPU： INTEL/AMD P166 以上

記憶體： 30MB+

硬碟： 30MB 未使用空間

1．4．2 軟體環境：

Windows 98

Windows 98se

Windows Me

Windows NT4 Workstation

Windows NT4 Server

Windows 2000 Pro

Windows 2000 Server

Windows 2000 Advance Server

Windows 2003 Server

Windows XP Home

Windows XP Pro

Windows XP (Home/Professional)

Windows Vista X32

Windows Vista X64

Windows Terminal Services

Internet Explorer version 5.5 以上

第二章　軟體安裝/移除與在線註冊

2．1 軟體安裝：

第一步　光盤自動安裝點擊安裝或執行安裝程式；

第二步　進入安裝程式歡迎介面，單擊【下一步】按鈕繼續安裝；

圖 2-1

第三步　【許可協議】窗口，請仔細閱讀軟體許可協議，並選擇【我同意】

選項，單擊【下一步】繼續安裝。如不接受該協議，將會退出安裝程式；

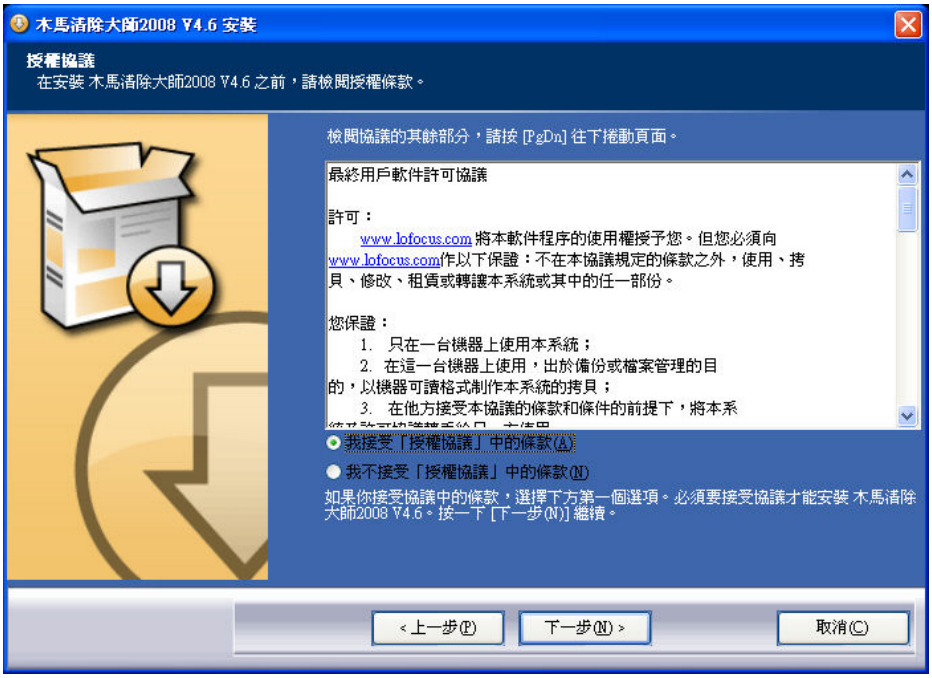

圖 2-2

第四步　在【選擇目標檔案夾】介面中選擇安裝木馬清除大師軟體的目標檔案夾（*默認安裝位置：C:\Program Files\BeatTrojan2008*），單擊【下一步】繼續安裝；

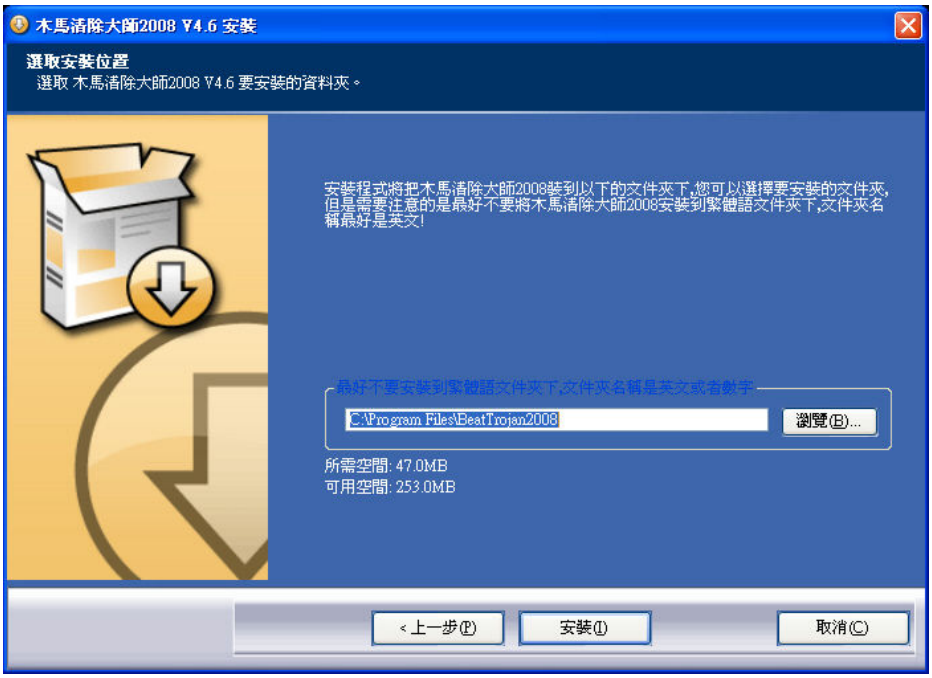

圖 2-3

第五步　安裝程式正將木馬清除大師檔案複製到硬碟裏；

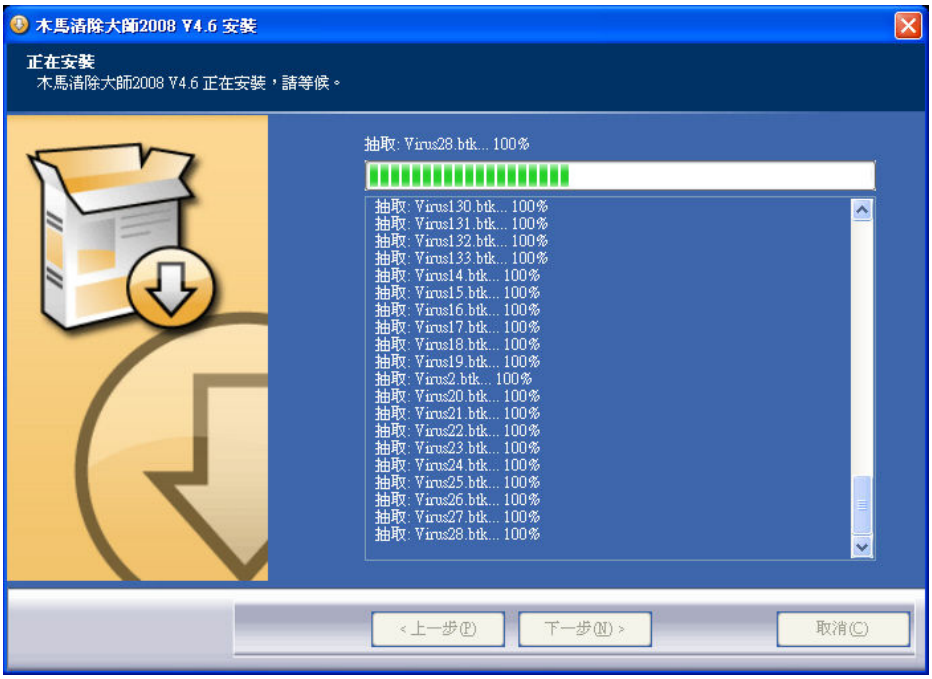

圖 2-4

第六步　檔案複製結束後，單擊【完成】結束安裝。

圖 2-5

2．2 軟體移除：

按開始->所有程式->木馬清除大師的「移除木馬清除大師」或者在控制臺的「新增或移除程式」中處理。

圖 2-6

確認移除，點擊【Yes】

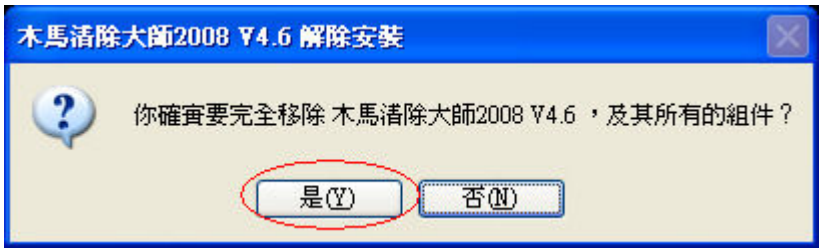

圖 2-7

點擊【是】系統重新啓動徹底刪除剩餘檔案，或點擊【否】在下一次啓動過程中刪除剩餘檔案。

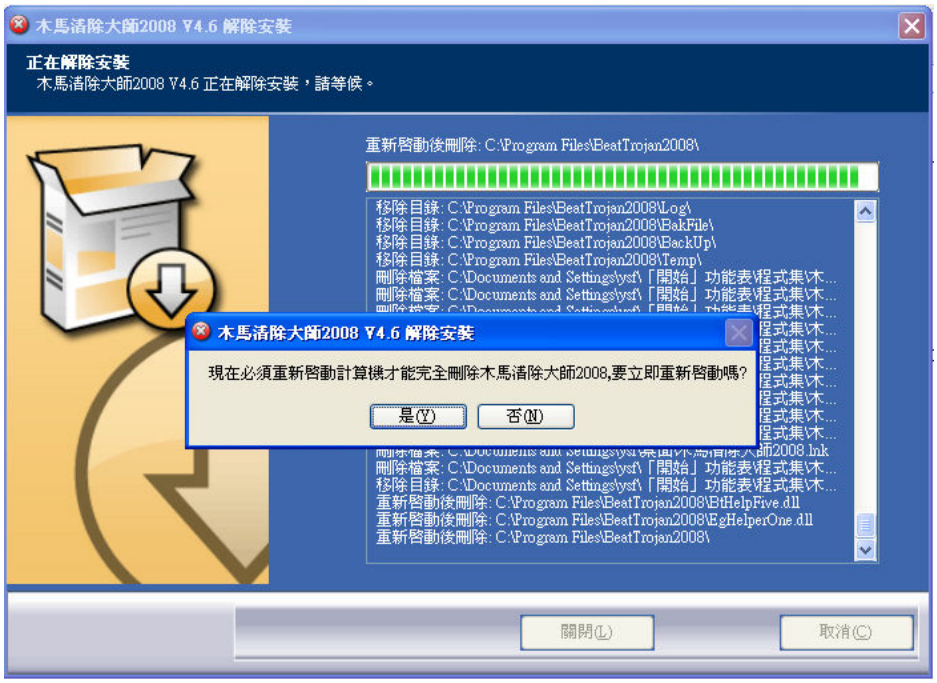

圖 2-8

2．3 軟體註冊：

木馬清除大師是商業軟體，這意味著您必須付費後才能使用全部功能。單擊【獲取註冊碼】將引導您至付費頁面，付費後您將在最短時間內獲得註冊碼。如果您已經獲得了使用者 ID 和註冊碼，請將其粘貼到下面的編輯框裡面，然後單擊【確認輸入】即可。注意：整個過程最好在連接網路的情況下進行，最後您必須重新啓動木馬清除大師以驗證註冊是否成功。

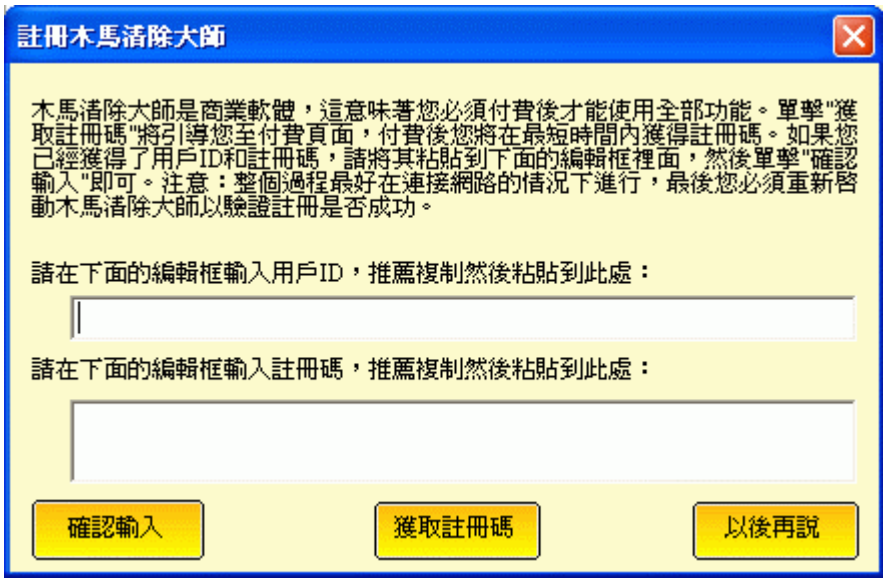

圖 2-9

註冊成功後，軟體主程式軟體狀態欄中會顯示軟體授權訊息和當前軟體病毒資料庫訊息。

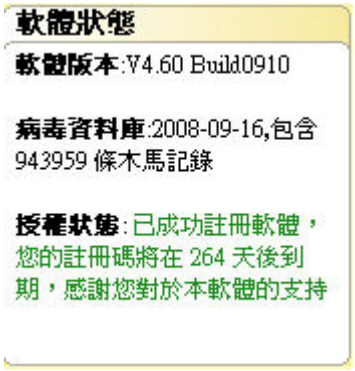

圖 2-10

第三章 木馬清除大師軟體使用

3．1 木馬清除大師軟體概述

木馬清除大師主要包含兩部分：**即時監控程式+主程式**

3・1・1 木馬清除大師即時監控程式

木馬清除大師即時監控程式爲系統後台執行，針對惡意程式等即時報警並按照預配的默認操作進行處理。能夠有效攔截當前流行的各種木馬、後門程式、流氓軟體等。

圖 3-1

3・1・2 木馬清除大師主程式（*控制臺*）

木馬清除大師控制臺爲木馬防護管理訊息、木馬防護設定的控制中心。提供完整的系統訊息、網路應用程式、日誌等訊息；木馬防護系統進行綜合的設定；啓動掃瞄引擎，並對全部磁碟進行完全查殺等操作。

3・2 木馬清除大師即時監控簡介

木馬清除大師一共有十四大即時監控，完全可以防止木馬，後門工具，流氓軟體，間諜程式安裝在用戶電腦上，這從根本上改變了以前中了木馬後再去掃瞄清除的模式，大大的提升了您電腦的安全性，隨時「*禦木馬於千里之外*」。

九大即時監控是什麼?

3・2・1 木馬即時攔截

木馬即時攔截是最有效的攔截木馬手段之一。當您執行一個程式，木馬清除大師將先截獲您要執行的程式檔案，然後對其進行安全掃瞄，如果發現是該程式

是木馬則阻止其執行並彈出警告窗口，交由您進行清除或阻止等操作，由此讓木馬根本沒有在您電腦上執行的機會。

3．2．2 記憶體即時監控

記憶體即時監控是防止木馬繞過本軟體的其他監控並在電腦內執行的最後一道防禦措施。只要在記憶體中發現活動木馬，木馬清除大師會彈出警告窗口，您可以清除該木馬，讓木馬無處藏身。

3．2．3 系統資料夾寫入監控

我們經過長期研究發現大部分木馬在執行的時候會釋放本身或者其他零件到系統資料夾下，系統資料夾寫入監控可以在任何檔案試圖在系統資料夾下建立時彈出警告窗口，您仔細分析檔案後可以選擇阻止其建立，相當於斬斷了木馬的左膀右臂。

3．2．4 系統資料夾執行監控

目前%90 以上的木馬都試圖在系統資料夾下執行，系統資料夾執行監控可以在任何程式試圖在系統資料夾下執行時會彈出警告窗口，您仔細分析檔案後可以選擇阻止其執行。

3．2．5 登錄檔即時監控

登錄檔即時監控包括兩大部分，其一是對登錄檔啓動項的監控，該監控能對超過十萬個登錄檔啓動項目進行監控，如果有木馬試圖修改登錄檔來實現隨系統

啓動，本軟體會第一時間會彈出警告窗口。其二是對登錄檔檔案關聯進行監控，如果有任何木馬試圖修改檔案關聯，您也可以即時阻止該操作。

3．2．6 IE 即時監控

IE 即時監控可以保護 IE 瀏覽器的多項設定不被修改，如果有任何程式試圖修改 IE 設定，軟體會彈出警告窗口，您可以即時阻止該操作。

3．2．7 重要系統檔案監控

Windows 有很多與系統安全密切相關的系統檔案，如 Win.ini，System.ini，hosts 等，這些檔案掌握著系統自身啓動程式，功能變數名稱 IP 轉換等重要配置訊息，系統檔案監控能保護這些檔案不被非法修改，如果有任何程式試圖修改系統檔案，軟體會彈出警告窗口，您可以查看「詳細訊息」並即時選擇阻止/忽略該事件。

3．2．8 敏感資料夾即時監控

目前大部分木馬爲了更好的隱蔽自己，大多將自己隱藏在系統資料夾下，系統資料夾下檔案眾多，只靠手工很難清除木馬。本監控即時監控系統資料夾，如果發現有害程式，軟體會彈出警告窗口，您可以即時清除該有害程式。

3．2．9 蠕蟲即時攔截

蠕蟲是傳播最快最廣的網路病毒，我們根據多年的經驗，總結出來了蠕蟲執行的基本規律。本監控會在任何檔案試圖執行時截獲該操作，然後判斷是否可疑，如果可疑，軟體會彈出警告窗口，您可以即時阻止執行該可疑程式。

3．2．10 程式強制終止監控

許多木馬爲了更好的隱藏和傳播自己,往往會關閉用戶電腦上的反病毒軟體,本監控會在一個進程被另一個進程結束的時候第一時間向您報告,您可以即時阻止或者允許該操作.注:該即時監控也屬於主動防禦欄目.

3．2．11 進程注入監控:

注入類隱藏木馬,是黑客近幾年較爲常用的木馬之一,它的主要特點是將自己或者自己的一部分注入到正常任務中,並且一般都是"winlogon.exe,csrss.exe"等 Windows 重要進程,來掩蓋其木馬的真身.這種木馬有難於發現,難於刪除的特點.本監控會在一個進程試圖寫入另一個進程內存或者創建遠程線程的時候,第一時間向您報告,您可以即時阻止或者允許該操作.注:該即時監控也屬於主動防禦欄目.

3．2．12 木馬側錄監控:

鈎子是 Windows 作業系統中非常重要的系統介面,用它可以截獲並處理送給其他應用程式的消息,來完成普通應用程式難以實現的功能.鈎子的種類很多,每種鈎子可以截獲並處理相應的消息,如鍵盤鈎子可以截獲鍵盤消息等.木馬就利用這個原理來盜取用戶輸入的網上銀行密碼,MSN 密碼,網路遊戲密碼等.本監控會在一個進程試圖安裝鈎子的時候第一時間向您報告,您可以即時阻止或者允許該操作.注:該即時監控也屬於主動防禦欄目.

3．2．13 網頁木馬監控:

網頁木馬是目前用戶中木馬的最常見渠道,目前全世界有 70%左右的網站都被黑客挂上了木馬,如果用戶使用沒有打最新安全更新的 IE 瀏覽器訪問這些被挂了馬的網站,木馬就會被自動下載並安裝到用戶的電腦上.本監控會攔截目前已經出現的所有網頁木馬,用戶可以即時阻止並清除.

3．2．14 USB 磁碟病毒監控:

USB 磁碟傳播是感染傳播型木馬傳播的主要途徑之一,這些木馬利用 Windows 的自動運行特點通過 USB 磁碟傳播自身,當用戶將 USB 磁碟插入電腦的時候,木馬就會自動運行.本監控可以自動檢測 USB 磁碟的插入,當發現有 USB 磁碟插入時,木馬清除大師會首先掃描 USB 磁碟上是否有病毒,如果有病毒會讓您直接清除.

3．3 木馬清除大師即時監控設定

雙擊系統托盤的即時監控圖標或者通過菜單選擇執行即時監控設定程式。

木馬清除大師即時監控設定介面一共分爲 5 部分：啓動設定，主動防禦設定,默認操作，隔離設定，按鈕部分。

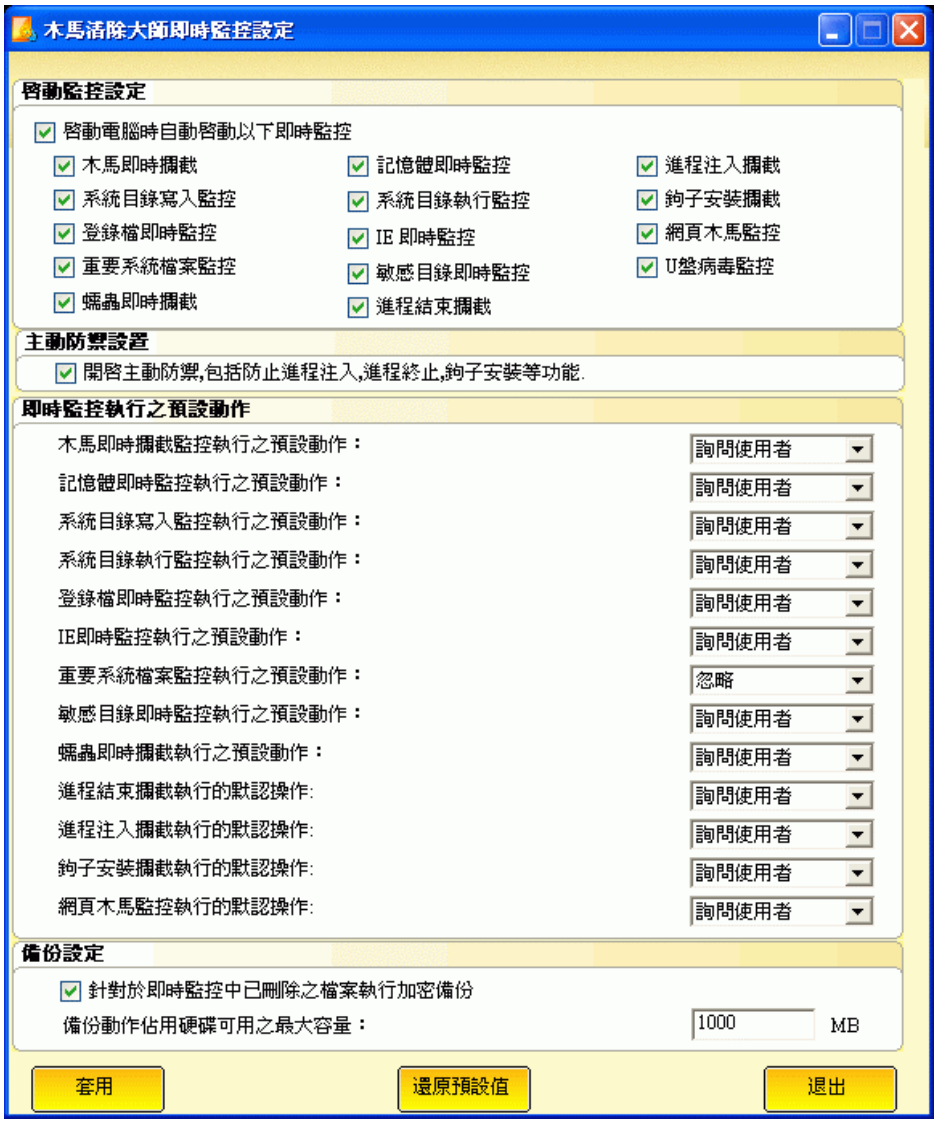

圖 3-2

3・3・1 啓動設定：

在頁面的上方您可以設定讓什麼監控隨系統啓動而啓動，默認所有監控全部自動啓動。

3．3．2 默認操作：

默認操作中所有監控依次排列，您可以設定當這些監控發生時需要執行什麼默認操作，直接從後面的組合框裡選擇即可，默認當監控到危害程式時，詢問用戶再執行相關操作。

3．3．3 隔離設定：

在這裡您可以設定是否加密隔離在即時監控中被刪除的檔案，同時可以設定允許隔離的最大硬碟空間。

3．3．4 按鈕部分：

●點擊【應用更改】將應用您的所有設定

●點擊【恢復設定】將恢復本軟體出品時候的設定

●點擊【退出】將退出設定程式

3．4 木馬清除大師即時監控規則設定

即時監控-規則設定—>系統資料夾執行，能夠反映系統資料夾執行程式的狀態。並可以通過【重新整理】、【添加】、【刪除】、【恢復默認】按鈕完成對執行程式監控狀態查詢/設定。其他項目可以通過同樣操作設定.

圖 3-3

3．5 木馬清除大師警告窗口

當有危害電腦安全的情況發生時，在本軟體系統托盤的位置會彈出一個警告視窗，視窗分爲 6 部分：標題、概述、具體訊息、輔助訊息、組合框、按鈕部分。

3．5．1 標題：

標題直觀地指示出了此次屬於什麼類型監控 。

3．5．2 概述：

概述在標題下面，將此次危害事件簡要描述。

3．5．3 具體訊息：

具體訊息反映了此次危害事件的主角，比如在登錄檔監控中添加一個啓動項目時候，該訊息將包含啓動項名稱，啓動項鍵值等。

3．5．4 輔助訊息：

點擊具體訊息旁邊的【詳細訊息】按鈕，會彈出一個輔助訊息框，裡面詳細描述了該檔案的所有訊息，並且提供極其實用的三個功能：

●定位檔案：直接定位到可疑檔案所在的資料夾，用戶可以直接對檔案做各種操作。

●複製檔案到：複製可疑檔案到用戶規定的資料夾，便於統一管理，大大方便了用戶的工作。

●在 Google 中查找：在用戶無法判定檔案是否正常的時候，就可以直接利用這個功能在 Google 這個全球最大的搜索引擎上搜索，可疑檔案的情況一目瞭然。

3．5．5 組合框：

組合框定義了您需要即時監控執行的操作。

3．5．6 按鈕部分：

●點擊【確定】將執行組合框裡面的操作，如果把「始終記住該項設定」前面的勾打上，則下次出現同樣的情況時，警告窗口將不再彈出，而是執行您此次選擇的操作。

●點擊【忽略】將忽略此次警告，希望慎用。因爲不對有害程式執行任何操作是相當危險的。

3・5・7 示例：

下圖顯示爲木馬清除大師即時監控程式提示重要系統檔案被修改。系統檔案被修改可以自動啓動程式，選擇預置操作「阻止」，並勾選「*對該項，始終記住此設定*」，並選擇【確定】。

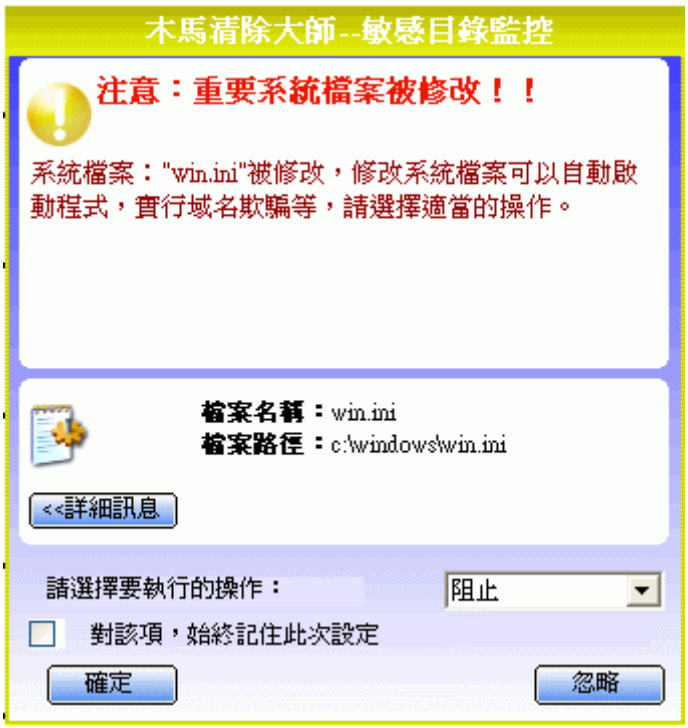

圖 3-8

下圖顯示系統檔案資料夾被寫入檔案。這個監控窗口同即時監控設定項對應。

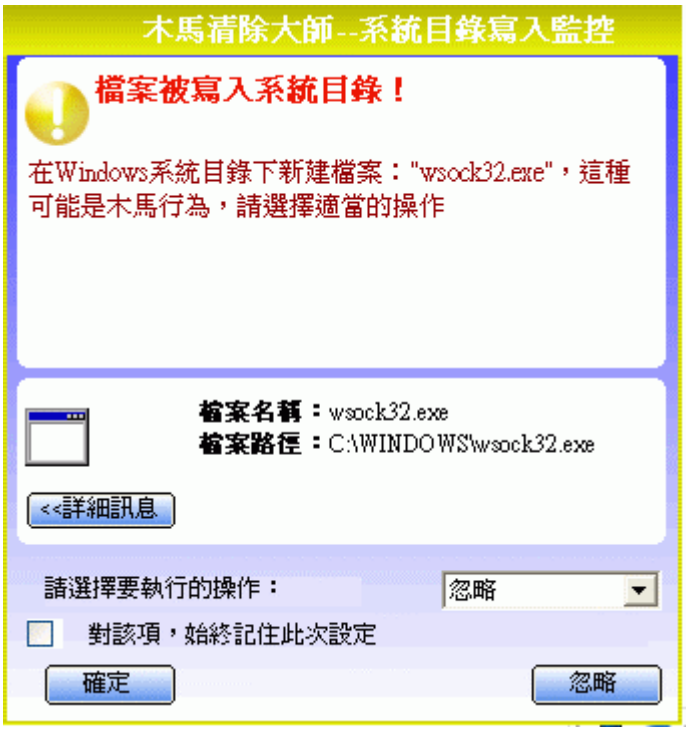

圖 3-9

下圖顯示有木馬入侵，木馬名爲：HackTool.Win32.Delf.oz。請選擇「清除木馬」並勾選「始終記住該設定」並選擇【確定】或者直接選擇【確定】。

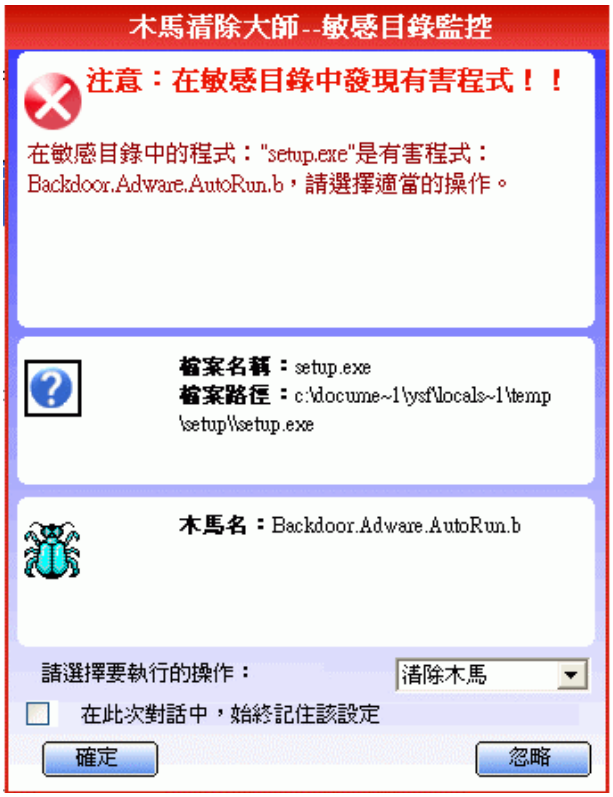

圖 3-10

下面圖顯示 IE 添加插件，有可能爲惡意程式。選擇【確定】操作。

圖 3-11

3．6 木馬清除大師主程式設定

木馬清除大師設定介面一共分爲兩大部分：基本設定，其他設定。

3・6・1 基本設定：

圖 3-12

a 檔案掃瞄類型：

●選擇掃瞄可執行檔案將掃瞄檔案擴展名爲.exe/.scr 的檔案

●選擇掃瞄動態連接庫檔案將掃瞄檔案擴展名爲.dll 的檔案

●選擇掃瞄壓縮檔案將掃瞄檔案擴展名爲.rar/.zip 的檔案

●選擇掃瞄所有檔案將掃瞄所有檔案而不在意檔案擴展名

b 檔案掃瞄規則：

●選擇使用智慧提速會大大加快掃瞄速度，但是對捆綁木馬檢測概率較低。

●選擇全面分析將減緩掃瞄速度，但是幾乎可以 100%查殺捆綁木馬，您如果對安全要求很高，建議選擇此項。

c 掃瞄完成後

該組定義了掃瞄硬碟完成後您需要本軟體執行的操作，比如您在睡覺的時候掃瞄，可以選擇掃瞄結束後關機。

3・6・2 其他設定：

圖 3-13

a 發現木馬後：

●選擇直接清除則軟體發現木馬後直接自動清除

●選擇忽略則軟體發現木馬後忽略該檔案，並繼續掃瞄。

b 隔離設定：

●選擇不隔離則軟體刪除木馬檔案後不進行隔離，這樣如果誤刪了檔案將不能被找回。

●選擇隔離則軟體刪除木馬檔案後進行加密保存，如果您覺得某個檔案是正常檔案，可以在主介面裡直接恢復

●默認隔離資料夾在軟體安裝資料夾的 Backup 資料夾下，您也可以點擊【瀏覽】按鈕手工選擇。

c 右鍵設定：

●選擇顯示則軟體將掃瞄菜單加入到系統上下文中，您可以隨時在您想掃瞄的檔案上面點右鍵，執行掃瞄。

●選擇不顯示則軟體將系統中的掃瞄菜單去除

d 報警設定：

●選擇不報警則軟體發現木馬後不發出報警音

●選擇報警則軟體發現木馬後會發出警告聲音

●本軟體已經自帶報警聲音，當然您也可以點擊【瀏覽】按鈕手工選擇

3．7 木馬清除大師掃瞄介面

木馬清除大師掃瞄介面一共分爲 5 部分：

掃瞄內容，掃瞄結果，動畫視窗，進度條，按鈕部分

圖 3-14

3・7・1 掃瞄內容：

●將「掃瞄記憶體」選上將執行對記憶體的快速掃瞄

●將「掃瞄 Cookies」選上將執行對 Cookies 的快速掃瞄

●將「掃瞄敏感資料夾」選上將執行對敏感資料夾的快速掃瞄

●將「掃瞄登錄檔」選上將執行對登錄檔的快速掃瞄

●將「掃瞄隱私項目」選上將執行對隱私項目的快速掃瞄

當您在選擇掃瞄內容時，在右邊都會顯示您當前選擇的內容，並且會給出預計掃瞄時間。

3・7・2 掃瞄結果：

掃瞄結果會在掃瞄頁面的最右邊顯示出來，掃瞄結果會隨著掃瞄進程的進行即時更新，如果發現有害程式，結果會以紅色的數字顯示，方便用戶查看。

3．7．3 動畫窗口：

動畫窗口在掃瞄內容下面，在掃瞄過程中不斷播放，使整個掃瞄在比較輕鬆的環境下進行。

3．7．4 進度條：

進度條分爲兩個部分，上面的進度條對應著當前內容的掃瞄進度，下面的進度條對應掃瞄總進程的進度，掃瞄進程一目瞭然。

3．7．5 按鈕：

●點擊【開始掃瞄】將執行掃瞄

●點擊【停止掃瞄】將停止掃瞄

●點擊【下一步】將進入對掃瞄結果頁面，如果發現的有害程式很多，請耐心等一會，結果會以列表的形式供用戶操作。

3．8 木馬清除大師掃瞄硬碟

木馬清除大師掃瞄硬碟介面一共分爲 4 部分：掃瞄內容，列表頁面，掃瞄進度，按鈕部分.

圖 3-15

3・8・1 掃瞄內容：

掃瞄內容以樹狀結構列出了您電腦的所有磁碟，您可以點擊前面的「+」號進入更深的資料夾，點擊復選框可以選擇掃瞄該資料夾，再次點擊則取消該資料夾。

3・8・2 列表頁面：

掃瞄結果會在掃瞄頁面依次顯示：

●第一列指出了有害程式檔案名

●第二列指出了有害程式路徑

●第三列指出了病毒名

●第四列指出了查殺狀態，如果顯示綠顏色的「清除成功」則表示清除成功，如果顯示紅顏色的「無法清除」則表示該檔案正在被系統使用，建議您到安全模式清除，或者用光碟或者軟盤進入 Dos 模式，直接手工刪除該檔案。

3．8．3 掃瞄進度：

●上面的訊息框會滾動顯示當前正在掃瞄的檔案

●左邊的訊息框會顯示已經掃瞄了多少檔案

●中間的訊息框會顯示發現了多少個木馬

●右邊的訊息框會顯示掃瞄耗費了多少時間

3．8．4 按鈕部分：

●點擊【開始掃瞄】將執行掃瞄

●點擊【停止掃瞄】將停止掃瞄

●點擊【另存爲】將保存當前的掃瞄結果

3．9 木馬清除大師掃瞄結果

木馬清除大師掃瞄結果介面一共分爲 5 部分：概述，列表頁面，幫助訊息，按鈕部分.

圖 3-16

3・9・1 概述：

在頁面的上方會向您報告發現了多少個有害程式或者隱私紀錄，方便您的統計。

3・9・2 列表頁面：

掃瞄結果會在掃瞄頁面依次顯示，木馬類包含了四列，隱私紀錄只有三列：

●第一列指出了有害程式類型

●第二列指出了有害程式路徑

●第三列指出了病毒名　注意*：如果是隱私紀錄則無此列*

●第四列指出了有害程式危險度，紅色代表到度危險，黃色代表中度危險，綠色代表輕度危險。點擊列表中的某一行，將在右邊的幫助訊息裡顯示相應的幫助內容。右鍵單擊列表中的一行，將彈出命令菜單，具體功能將在下面描述。

3・9・3 幫助訊息：

幫助訊息顯示您選擇的有害項目的具體訊息，您可以瞭解到該有害項目的大體危害，並且能得到我們的建議。

3・9・4 按鈕部分：

●點擊【選擇全部】將全部選擇列表頁面的所有項目

●點擊【取消全部】將全部取消列表頁面的所有項目

●點擊【刪除】將刪除您選擇的項目

●點擊【返回掃瞄】將返回掃瞄頁面

3．9．5 菜單功能：

菜單功能基本與頁面底部的按鈕功能一致：

●點擊「清除該有害項目」與按鈕部分的【刪除】功能一致

●點擊「選擇全部」與按鈕部分的【選擇全部】功能一致

●點擊「取消全部」與按鈕部分的【取消全部】功能一致

●點擊「保存掃瞄結果」將保存當前的掃瞄結果

●點擊「幫助」將打開幫助手冊

3．10 木馬清除大師進階工具

木馬清除大師進階工具包含七大功能，在原來的功能上增強不少，可以輕鬆斬殺流氓間諜軟體，是您診斷系統的強有力助手。

3．10．1 啓動管理器：支援 Win9x\Me\Nt\2000\Xp\2003

可以查看系統的啓動項目，選擇您要刪除的啓動項，點擊【刪除】按鈕刪除該項。

啓動項目：隨作業系統啓動而啓動的應用程式

圖 3-17

3．10．2 檔案關聯：支援 Win9x\Me\Nt\2000\Xp\2003

可以查看系統的檔案關聯，並且可以檢查檔案關聯是否正常，如果不正常就恢復，使檔案關聯型木馬無用武之地.如果您發現有檔案關聯不正常，選擇此項後，點擊【恢復】按鈕即可。

檔案關聯：指出某種檔案名應該由哪個程式打開。如「.txt」檔案的檔案關聯項目一般是「系統資料夾\notepad.exe %1」。

圖 3-18

3．10．3 進程管理：支援 Win9x\Me\Nt\2000\Xp\2003

進程管理是一個很強大的工具，可以查看系統裡進程的進程名、進程 ID、進程路徑、調用模塊，進程所對應檔案的詳細訊息，並且可以直接定位檔案。您可以使用它關閉無法在 Windows 工作管理員裡關閉的進程。

圖 3-19

3．10．4 網路活動：支援 Win2000\Xp

網路活動可以顯示什麼進程打開了什麼埠，這是對 DOS 命令「Netstat/an」的加強版，可以直觀的顯示什麼進程打開了什麼埠，並且可以關閉懷疑的進程(比如 XX 進程打開了 7626 埠，您可以根據實際情況將其終止)。

埠：電腦之間連接時使用的通道，可以被程式打開並且建立與其他電腦的連接，用數字表示，一個程式往往只打開特定的埠，如冰河打開 7626 埠。

圖 3-20

3・10・5 服務管理：支援 WinNt\2000\Xp\2003

可以查看系統執行了什麼服務和服務的詳細訊息，選擇一個服務後(即點擊列表中的一項)，點擊【啓動】或【停止】按鈕啓動或停止您指定的服務。

服務：服務是 Win9x 以後的作業系統才引入的東西，它是一種在後台執行的應用程式類型，每個服務都有特定的權限。

圖 3-21

3．10．6 IE 插件：支援 Win9x\Me\Nt\2000\Xp\2003

可以查看 IE 瀏覽器加載了哪些插件，往往很多莫名其妙的廣告都是這些插件搞的鬼，請仔細查看哪些插件不是您需要的並選擇刪除。

圖 3-22

3．10．7 IE 設定支援 Win9x\Me\Nt\2000\Xp\2003

如果您發現自己每次上網就自動連接到一個陌生的網站，並且「工具」中的「Internet 選項」中的更換主頁是灰色的無法使用，想改登錄檔發現登錄檔編輯器也被鎖定無法使用，那麼您可以使用這個工具恢復 IE 的默認設定和一系列登錄檔被修改後的症狀。點擊【修復】按鈕來執行修復過程。可以點擊介面下面的列表框一項，然後點擊【刪除】按鈕來刪除在 IE 中點擊右鍵時出現的項目。

圖 3-23

3．11 木馬清除大師智慧升級

木馬清除大師線上升級程式非常智慧,每日都會自動連接網路進行升級,淡然您可以也可以手工點【升級】按鈕實現升級。

圖 3-24

點擊【開始升級】，進行病毒資料庫或者程式組件下載。

圖 3-25

升級程式正在從伺服器下載升級程式或者病毒資料庫檔案。

圖 3-26

升級完畢，升級程式提示升級操作需要重新啓動主程式和即時監控程式，點擊【確認】重新啓動防護程式。

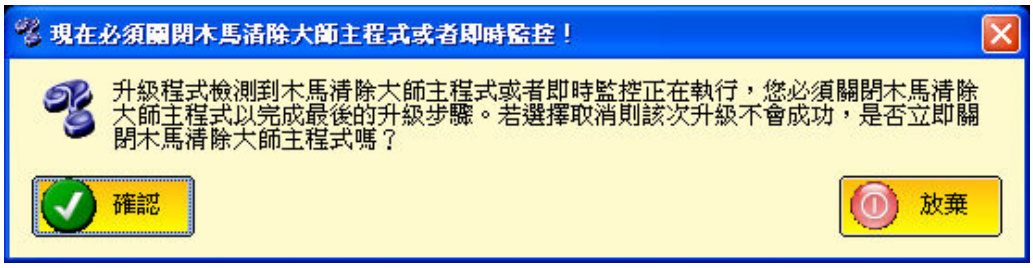

圖 3-27

3．12 木馬清除大師隔離

木馬清除大師隔離介面一共分爲 2 部分：列表頁面、按鈕部分；

圖 3-28

3・12・1 列表頁面：

被隔離的程式會在隔離頁面依次顯示：

●第一列指出了隔離前原始檔案的檔案名

●第二列指出了刪除原因，比如在掃瞄中刪除還是被即時監控刪除

●第三列指出了時間，表示該檔案是在什麼時候被隔離

●第四列指出了隔離前原始檔案的檔案路徑

3・12・2 按鈕部分：

●點擊【選擇全部】將全部選擇列表頁面的所有項目
●點擊【取消全部】將全部取消列表頁面的所有項目
●點擊【恢復】將從被選擇的隔離檔案恢復到原始的有害程式
●點擊【刪除】將徹底刪除被選擇的隔離檔案，以後將不能恢復該檔案

附件一：

本軟體的查殺病毒名稱遵循國際慣例，比如 Trojan.***，BackDoor.***，HackTool.***，Password.***，想知道這些術語代表什麼含義請仔細查看以下訊息：

1、什麼是木馬(Trojan.***)？

木馬，也稱特洛伊木馬，名稱源於古希臘的特洛伊神話故事，傳說希臘人圍攻特洛伊城，久久不能得手。後來有人想出了一個木馬計，讓士兵藏匿於巨大的木馬中。大部隊假裝撤退而將木馬丟棄於特洛伊城下，讓敵人將其作爲戰利品拖入城內。木馬內的士兵則乘夜晚敵人慶祝勝利、放鬆警惕的時候從木馬中爬出來，與城外的部隊裡應外合而攻下了特洛伊城。木馬的危害性在於它對電腦系統強大的控制和破壞能力，竊取密碼、控制系統操作、進行檔案操作等等，一個功能強大的木馬一旦被植入您的電腦，攻擊者就可以像操作自己的電腦一樣控制您的電腦，甚至可以遠程監控您的所有操作。

2、什麼是後門工具(BackDoor.***)？

有些軟體程式員有意識地設計了後門程式，作爲惡意訊息傳播過程中的「內應」。後門程式更像是潛入電腦中的小偷，允許不法分子繞過常規的鑒定程式非法訪問電腦。

3、什麼是黑客工具(HackTool.***)？

黑客工具是黑客用來入侵其他電腦的工具，它既可以作爲主要工具，也可以作爲一個跳板工具安裝在電腦上供黑客侵入電腦系統時使用。

4、什麼是蠕蟲(Worm.***)？

蠕蟲的公有特性是通過網路或者系統漏洞進行傳播，很大部分的蠕蟲病毒都有向外發送帶毒郵件，阻塞網路的特性。比如衝擊波阻塞網路，小郵差(髮帶毒郵件)等。

5、什麼是廣告軟體(Adware.***)？

Adware 就是傳統意義上的廣告軟體，出於商業目的，廣告軟體經常在未經用戶許可的情況下，彈出讓用戶非常反感的廣告，並偷偷收集用戶個人訊息，轉交給第三方。

6、什麼是間諜軟體(Spyware.***)？

間諜軟體是一種能夠在電腦使用者不知不覺的情況下，在用戶的電腦上安裝「後門程式」的軟體。雖然那些被安裝了「後門程式」的電腦使用起來和正常電腦並沒有什麼太大區別，但用戶的隱私數據和重要訊息會被那些「後門程式」所捕獲，這些訊息將被發送給互聯網另一端的操縱者，甚至這些「後門程式」還能使黑客操縱用戶的電腦，或者說這些有「後門」的電腦都將成爲黑客和病毒攻擊的重要目標和潛在目標。

7、什麼是密碼大盜(Password.***)？

密碼偷竊程式是現在互聯網上對個人用戶危害最大的木馬程式之一，黑客出於經濟利益目的，安裝此類程式以獲取用戶的機密訊息，如網上銀行賬戶、網路

遊戲帳號/密碼、QQ/MSN 密碼等，這是在互聯網上給用戶的真實財富帶來最大威脅的後門程式。

8、什麼是鍵盤紀錄程式(KeyLogger.***)？

鍵盤紀錄程式是危害性非常大的一種木馬程式，它常常在用戶輸入機密訊息（如 QQ 密碼、網路遊戲密碼及個人隱私）的時候紀錄下用戶的按鍵，並將其保存下來通過電子郵件或者其他方式發送給黑客。

9、什麼是病毒(Virus.***)？

病毒程式的最大特點是具有主動傳染性。病毒可以侵入到整個系統使其受到感染，而每個受感染的程式又可能成爲一個病毒源，繼續將病毒傳染給其他程式。所以病毒程式會嚴重消耗電腦資源、破壞作業系統、硬體配置數據和程式檔案，但是並不會引起用戶機密訊息的洩露。

10、什麼是惡作劇程式(Joker.***)？

惡作劇的公有特性是本身具有好看的圖標來誘惑用戶點擊，當用戶點擊這類病毒時，病毒會做出各種破壞操作來嚇唬用戶。其實病毒並沒有對用戶電腦進行任何破壞。如：女鬼病毒。

11、什麼是捆綁程式(Binder.***)？

捆綁病毒的公有特性是病毒作者會使用特定的捆綁程式將病毒與一些應用程式如 QQ，IE 捆綁起來，表面上看是一個正常的檔案，當用戶執行這些捆綁了病毒的程式時，表面上執行的是這些應用程式，實際上捆綁在一起的病毒同時執行，從而給用戶電腦訊息造成危害。